UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

BYTEMARK, INC.,	§	
	§	
Plaintiff,	§	
	§	
v.	§	**CIVIL ACTION NO. 1:17-cv-01803**
	§	**(PGG)**
XEROX CORP., ACS TRANSPORT SOLUTIONS, INC., XEROX TRANSPORT SOLUTIONS, INC., CONDUENT INC., and NEW JERSEY TRANSIT CORP.,	§	**ECF CASE**
	§	
	§	
	§	
	§	
	§	
Defendants.	§	
	§	
	§	
	§	
	§	

DEFENDANTS' REPLY IN SUPPORT OF ITS MOTION TO COMPEL AND MOTION FOR PROTECTIVE ORDER

Table of Contents

I. Introduction

There is no dispute that a trade secret plaintiff must disclose its trade secrets with ***reasonable*** particularity prior to discovering a defendant's confidential information. Rather, the dispute is whether Bytemark's broad categorizations in its complaint or, alternatively, its promise to produce "all" its source code, is sufficient at this stage of the case. It is not. Multiple New York courts have held that generic descriptions of categories, like those in Bytemark's complaint, fail to describe trade secrets with sufficiently ***reasonable*** particularity. And Bytemark has found no authority to support is position that a voluminous source code production satisfies its obligations because it does not.

Despite Defendants' repeated attempts at compromise, Bytemark is unwilling to identify its trade secrets in greater detail than the broad, amorphous categories in its complaint. Instead, it now asks this Court for permission to peek behind Defendants' curtain, examine in detail the highly confidential inner workings of Defendants' products, and only then identify the information over which it alleges trade secret protection. Court after court has recognized the inherent unfairness of such an approach. And for this reason, court after court has required a trade secret plaintiff to identify its trade secrets with ***reasonable*** particularity prior to accessing a defendant's confidential information. Bytemark is capable of doing so now, and until it does, the Court should preclude further discovery into Defendant's highly confidential information. This is what Defendants' Motion requests, and this is what the great weight of authority compels.

II. Factual Background

The events preceding this dispute have been fully developed, both in this Motion and in Bytemark's co-pending Motion to Compel. Two key points, however, are worth reiterating.

First, on October 23, 2018 Defendants served the first discovery requests in this case. Defendants First Set of Interrogatories requested, among other things, that Bytemark identify its alleged trade secrets. Mot. at Ex. B (Defendants First Set of Interrogatories) at Interrogatory 1. Defendants First Set of Requests for Production requested, among other things, that Bytemark produce documents identifying and embodying its alleged trade secrets. Mot. at Ex. C (Defendants First Set of Requests for Production) at, *e.g.*, RFP 1-6. To this day, Bytemark has failed to substantively respond to any of these requests.

Second, over the past two years, the parties have attempted to reach a compromise that would avoid burdening this Court. Bytemark recasts itself as the reasonable party offering repeatedly to allow Defendants to inspect its trade secrets. What Bytemark fails to mention, however, is that it retracted these offers before Defendants could arrange for inspection. And all its offers required Defendants to concede that Bytemark could wait until the end of discovery to identify its trade secrets. Bytemark's last word on the subject makes its position very clear: Bytemark is "not willing to produce such a [trade secret disclosure] document" and it will respond to Defendants' request for an identification of trade secrets "**at the conclusion** of other discovery. . . ." *See, e.g.*, Ex. E at 2 (emphasis added). Because Bytemark will not identify its trade secrets, Defendants saw no path forward other than Court intervention. Defendants simply request what they are entitled to; a reasonably particular identification of Bytemark's alleged trade secrets followed by full and open discovery from both sides.

III. Argument

A. Both parties' authorities confirm that Bytemark must identify its trade secrets with reasonable particularity early in the case.

Defendants' Motion seeks an order compelling Bytemark to identify its trade secrets with reasonable particularity prior to any further discovery into Defendants' highly confidential information. Bytemark refuses even though "Bytemark is aware of what confidential and proprietary information it has shared with Defendants." Resp. at 8. In sum, Bytemark wants to withhold all details of its trade secrets until it can peruse Defendants' source code and other confidential information. This is not the law.

1. Bytemark has failed to identify its trade secrets with reasonable particularity as is required by court precedent.

Recognizing the weakness of its position, Bytemark's main response is to suggest it has sufficiently identified its trade secrets in its complaint. But Bytemark's broad characterization of its alleged trade secrets as all aspects of a "mobile ticketing system" is anything but reasonably particular. Rather, it is precisely the type of broad, categorical trade secret disclosures that New York district courts will ***not*** tolerate. For example, Bytemark's lead case, *Uni-Sys.*, recognizes "that generic descriptions of categories are insufficient to provide defendants with information sufficient to satisfy the 'reasonable particularity' standard." *Uni-Sys., LLC v. U.S. Tennis Ass'n*, No. 17CV147, 2017 WL 4081904, at *4 (E.D.N.Y. Sept. 13, 2017) (citations omitted).

In fact, Bytemark's disclosure is exactly what *Uni-Sys* rejects. Bytemark's complaint recites generic descriptions of categories that encompasses every aspect of a mobile ticketing system, such as "mobile ticket development technology and know-how," "back-end application and system management, maintenance, and service," and "pricing, sales initiatives and profit generation paradigm." *See* Resp. at 9. Bytemark's disclosure is akin to Tesla describing its trade secrets as "electric car technology, including batteries, motors, electronics, and the related know-how, systems, and pricing." Such a description leaves a defendant to guess what within the broad category of "electronics" or "batteries" constitutes the trade secrets. The same is true of Bytemark's disclosure. Defendants must guess what part of mobile ticketing the alleged trade secrets relate to, which is especially troubling given that mobile ticketing (like electronics and batteries) has been in the public domain for decades. *See, e.g.*, plusdial.net/highlights (stating that its first mobile ticket was sold in 2001, and its mobile ticketing pilot started in 2002); USP 7,520,427 titled "Method of Operating a Ticketing System" filed on November 21, 2005. As Bytemark failed to "describe the subject matter of [its] trade secret with sufficient particularity to separate it from matters of general knowledge in the trade or of special knowledge of those persons skilled in the trade," its disclosure is insufficient. *ValveTech, Inc. v. Aerojet Rocketdyne, Inc.*, No. 17-CV-6788-FPG, 2019 WL 4688737, at *3 (W.D.N.Y. Sept. 26, 2019).

The *Uni-Sys* ruling does not stand alone. Other courts in the Southern District of New York have repeatedly found disclosures like Bytemark's insufficient to define a trade secret with reasonable particularity. *See, e.g., Big Vision Private, Ltd. v. E.I. Du Pont De Nemours & Co.*, 1 F.Supp. 3d 224, 258 (S.D.N.Y. Mar. 3, 2014). For example, the *Big Vision* court surveyed cases across the country and concluded that they all require some amount of specificity beyond "general allegations and generic references to products." *Id.* at 259. The court then held that "several district courts within this Circuit have adopted this particularity requirement, and this Court now joins them." *Id.* Thus, consistent with Southern District of New York case law, Bytemark must do more than provide "general categories of information," "general allegations," and "generic references to products." *Id.* at 259; *see also Heyman v. AR. Winarick, Inc.*, 325 F.2d 584, 590 (2d Cir. Dec. 24, 1963) (holding that a trade secret description of a quaternary and non-toxic surface agent used in a fingernail hardener was too vague and indefinite); *DS Parent, Inc. v. Teich*, No. 5:13-CV-1489 LEK/DEP, 2014 WL 546358, at *8 (N.D.N.Y. Feb. 10, 2014) (finding a trade secret description of "science and engineering of [] liquid coating systems . . ., including the empirical testing and trial-and error" performed by the trade secret plaintiff to be an insufficient disclosure).

2. Bytemark is capable of describing its trade secrets with reasonable particularity.

Bytemark has no excuse for its failure to sufficiently identify its alleged trade secrets. To have a Rule 11 basis for asserting a trade secret claim, it must know which trade secrets form the basis of that claim. In fact, the elements of Bytemark's the Defend Trade Secrets Act ("DTSA"), New York common law, and New Jersey Trade Secret Act claims require the trade secret "owner [to] . . . ha[ve] taken reasonable measures to keep such information secret." 18 U.S.C. § 1839(3); *see also E.J. Brooks Co. v. Cambridge Sec. Seals*, 31 N.Y.3d 441, 80 N.Y.S.3d 162, 105 N.E.3d 301, 310 (2018) (New York law); N.J. Stat. Ann. 56:15-2 (New Jersey Trade Secrets Act). How can Bytemark aver that it kept the information secret if it can't even identify what that information is? Indeed, Bytemark concedes that it "is aware of what confidential and proprietary information it has shared with Defendants." Resp. at 9. It simply refuses to tell Defendants. Bytemark's motivation for withholding its alleged trade secrets is simple: Bytemark wants to tailor its broad allegations to the specific material it finds in Defendants' confidential information. But this is the very reason courts from this jurisdiction and others have required, as a matter of course, that trade secret plaintiffs identify their trade secrets with reasonable particularity prior to discovery. *See* Mot. at 7-10.

3. Bytemark's trade secret disclosure must occur early in the case.

Bytemark rejects this well-established precedent, suggesting it should be allowed to withhold a sufficient trade secret disclosure until "it has had a **full** opportunity to conduct discovery of the accused systems." Resp. at 12 (emphasis added). Again, this is not the law. Bytemark must define its trade secrets with reasonable particularity early in the case. New York courts are unequivocal on this point. In *MSCI*, the court held that "the law requires that a trade secret plaintiff identify trade secrets with reasonable particularity **early in the case**." *MSCI Inc.*

v. Jacob, 36 Misc. 3d 211, 213, 945 N.Y.S.2d 863, 865 (Sup. Ct. 2012) (emphasis added). The *DS Parent* case also joined in this reasoning. *DS Parent*, 2014 WL 546358 at *8 (citing *MSCI*). Trade secret treatises likewise support early trade secret identification. *See* 3 Milgram on Trade Secrets § 14.02 ("[I]t is essentially necessary for a plaintiff to identify its trade secrets before the defendant proceeds with disclosure of its confidential information.").

Bytemark's only retort is to argue that the facts of another case, *Xerox Corp. v. International Bus. Machs. Corp.*, support rewriting *MSCI's* requirement to disclose trade secrets "early in the case" as "after extensive discovery." Resp. at 15. This is nonsensical. In *MSCI*, the court ruled that the trade secrets must be identified "early in the case." *MSCI*, 36 Misc. 3d at 213. This is the opposite of a trade secret disclosure submitted "after extensive discovery." More importantly, the *Xerox* case supports early—rather than late—trade secret disclosure. *See Xerox Corp. v. International Bus. Machs. Corp.*, 64 FRD 367, 371-72 (S.D.N.Y. 1974) (holding that without a sufficient trade secret disclosure, "neither the court nor the parties can know, with any degree of certainty, whether discovery is relevant or not").

Even Bytemark's *Sit-Up* case supports this conclusion, as that court held it was "unfair . . . to the defendants to conduct discovery without knowing what the assertions are." *Sit-Up Ltd. v. IAC/InterActiveCorp.*, No. 05 CIV. 9292 (DLC), 2008 WL 463884, at *7 (S.D.N.Y. Feb. 20, 2008). To hold otherwise prevents Defendants from "testing whatever the plaintiff's theory is" during discovery. *Id.* at *15-16. As Bytemark's trade secret description is not reasonably particular, this Court should require a more detailed disclosure prior to Defendants' production of highly-confidential information and source code.

B. Bytemark's offer to produce "all" of its source code does not satisfy Bytemark's obligation.

Bytemark's offer to provide **all** of its source code as a trade secret disclosure also fails to provide a reasonably particular trade secret disclosure. In *PaySys*, the plaintiff stated that its trade secrets included its source code, which "consist[s] of millions of lines of source code with diverse functionality." *PaySys Int'l, Inc. v. Atos Se*, No. 14-CV-10105 (KBF), 2016 WL 7116132, at *11 (S.D.N.Y. Dec. 5, 2016). The *PaySys* court noted that "plaintiff has sought to shift the burden to defendants to prove what is not [a trade] secret." *Id.* at *28. This scenario "is the reverse of what the law requires." *Id.* Similarly, the *MSCI* case held that "providing defendants with plaintiffs' 'reference library' to establish what portions of their source code are in the public domain shifts the burden to defendants to clarify plaintiffs' claim. . . . Hence, it is insufficient." *MSCI*, 36 Misc. 3d at 865-66. Bytemark's solution to "produc[e] all of the source code and confidential information" and then require Defendants to dig through thousands of pages and millions of lines of code to guess its trade secrets is therefore improper and must be rejected. Resp. at 13.

C. This Court's precedent supports compelling identification of Bytemark's trade secrets.

Bytemark relies on Local Civil Rule 33.3 in an attempt to shirk its obligation to identify its alleged trade secrets with reasonable particularity. There is precedent, however, for requiring trade secret disclosures via interrogatories. In *Ferguson v. Ferrante*, the Southern District of New York heard a motion to compel regarding interrogatories much like those at issue in this case. No. 13 CIV. 4468 VEC, 2014 WL 1327968, at *2 (S.D.N.Y. Apr. 3, 2014). The defendants in *Ferguson* served interrogatories seeking "information relating to [plaintiff's] claims against the defendants for the misappropriation and conversion of trade secrets." *Id.* The *Ferguson* plaintiff had previously refused to answer these interrogatories. *Id.* After recounting the limitations imposed by Local Rule 33.3, the *Ferguson* court noted that the plaintiff's complaint did not "clarify 'with particularity the specific 'trade secrets and confidential business information' . . . that [defendants] allegedly appropriated or converted.'" *Id*. Next, the court recounted "the importance of pleading trade secrets with particularity; without knowing the specific secrets at issue, the defendants run the risk of re-using the secrets and the Court is unable to evaluate whether and to what extent they are doing so." *Id*. (citing *Big Vision*, 1 F. Supp. 3d at 257). Because it is important that a plaintiff identify its trade secrets with particularity, the Southern District Court ordered the plaintiff to answer the interrogatories and "particularly [] identify the alleged stolen trade secrets." *Id*.

Just like in *Ferguson*, Defendants' respectfully request that the Court order Bytemark to identify with reasonable particularity its alleged trade secrets, either via a compelled response to Interrogatory No. 1 (as in *Ferguson*), or via specific trade secret disclosures (as in multiple cases cited herein). Bytemark can articulate no reason why such a disclosure would burden it in any way. On the contrary, as multiple courts have held, such a disclosure will protect Defendants, streamline litigation, and prevent Bytemark's trade secrets from being a moving target throughout discovery.

D. A protective order is appropriate here.

Bytemark fails to undermine the ample good cause that exists for a protective order. Defendants will suffer a "clearly defined, specific and serious injury" in the absence of a protective order. *Qube Films Ltd. v. Padell*, No. 13-CV-8405, 2015 WL 109628, at *2 (S.D.N.Y. Jan. 5, 2015). This injury includes the inherent unfairness of allowing Bytemark to mold its broad trade secrets to Defendants confidential information, the inefficiencies of allowing Bytemark to conceal its trade secrets, and the continued disputes that will arise over Bytemark's failure to define its claims. On the other hand, Bytemark has articulated no credible injury it would suffer if the protective order is granted. Bytemark complains that Defendants' requested protective order "would bar Bytemark from obtaining highly relevant and crucial evidence." Resp. at 8. It would not. Bytemark will receive all the documents and information to which it is entitled under the Federal Rules and the Rules of this Court. Defendants' simply request that Bytemark first identify its trade secrets with reasonable particularity as required by the overwhelming majority of courts that address this issue. *See* Mot. at 7-10.

More importantly, the burden for Bytemark to gain access to the information it seeks is minimal. Bytemark knows its alleged trade secrets, and it knows what has been communicated to Defendants. Resp. at 9. It could, with little effort, identify its trade secrets with reasonable particularity. Fears that a disclosure would limit Bytemark's flexibility in this case are unwarranted. A response to Defendants' Interrogatory No. 1, or a trade secret disclosure ordered by the Court, could and *should* be amended as discovery progresses—the disclosure is just a starting point to streamline litigation and prevent unfairness. *See, e.g.*, Fed. R. Civ. P. 26(e). As case after case makes clear, Bytemark only needs to identify its trade secrets with sufficient detail to protect against unfairness, frame discovery, and permit Defendants to develop well-reasoned defenses. *See, e.g.*, *Sit-Up*, 2008 WL 463884, at *6 (finding trade secrets must be specified throughout litigation "so that the defendant can defend himself adequately against claims of trade secret misappropriation, and can divine the line between secret and nonsecret information"). Therefore, a protective order is warranted until Bytemark identifies its trade secrets with reasonable particularity.

IV. **Conclusion**

For these reasons, Defendants respectfully request that the Court grant its Motion to Compel and Motion for Protective Order.

Dated: January 6, 2021

Respectfully submitted,

/s/ Ashley N. Moore
Ashley N. Moore (admitted *pro hac vice*)
David Sochia (admitted *pro hac vice*)
Douglas A. Cawley (admitted *pro hac vice*)
Marcus L. Rabinowitz (admitted *pro hac vice*)

MCKOOL SMITH, P.C.
300 Crescent Court, Suite 1500
Dallas, Texas 75201
Tel: (214) 978-4000
Fax: (214) 978-4044
amoore@mckoolsmith.com
dsochia@mckoolsmith.com
dcawley@mckoolsmith.com
mrabinowitz@mckoolsmith.com

David R. Dehoney (4616595)
MCKOOL SMITH, P.C.
One Manhattan West
395 9th Avenue, 50th Floor
New York, New York 10001
Tel: (212) 402-9424
Fax: (212) 402-9444
ddehoney@mckoolsmith.com

Attorneys for Defendants